



Attorney's Docket No.: 006331.P008

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Dong-Hwan Shin, et al.)
) Examiner: Not Yet Assigned
Application No.: 10/685,881)
) Art Unit: 2621
Filed: October 14, 2003)
)
For: APPARATUS AND METHOD FOR)
PREVENTING FORGERY/)
ALTERATION OF THE DATA)
RECORDED BY DIGITAL VOICE)
RECORDER)
_____)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF PRIORITY PAPERS

Dear Sir:

In support of the claim for priority under 35 U.S.C. § 119, Applicant encloses
herewith a certified copy of the priority foreign application listed below:

<u>Serial No.</u>	<u>Date of Application</u>	<u>Country</u>
10-2002-0062768	10/15/2002	Republic of Korea

First-Class Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service as first-class mail with sufficient postage in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C., 20231 on

March 12, 2004
Date of Deposit

Linda K. Brost

Name of Person Mailing Correspondence


Linda K. Brost March 12, 2004
Signature Date

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: March 12, 2004

A handwritten signature in dark ink, appearing to read "Stephen M. De Klerk", is written over a horizontal line.

Stephen M. De Klerk

Reg. No. 46,503

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(408) 720-8300

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원번호 : 10-2002-0062768
Application Number

출원년월일 : 2002년 10월 15일
Date of Application OCT 15, 2002

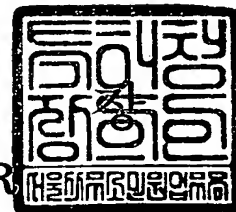
출원인 : (주)마크텍 외 1명
Applicant(s) MARKTEK INC., et al.



2003 년 10 월 02 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002. 10. 15
【발명의 명칭】	디지털 음성 저장 장치에 저장된 데이터의 인증 및 위/변조를 방지하기 위한 장치 및 방법
【발명의 영문명칭】	APPARATUS FOR AUTHENTICATION, PREVENTION OF FORGERY/ALTERATION OF THE DATA RECORDED BY DIGITAL VOICE RECORDER AND METHOD THEREOF
【출원인】	
【명칭】	(주)마크텍
【출원인코드】	1-2000-041196-8
【출원인】	
【명칭】	주식회사 마크애니
【출원인코드】	1-1999-026375-7
【대리인】	
【명칭】	특허법인코리아나
【대리인코드】	9-2001-100001-3
【지정된변리사】	변리사 박해선, 변리사 이윤민, 변리사 이철
【포괄위임등록번호】	2001-037861-3
【포괄위임등록번호】	2001-018108-8
【발명자】	
【성명의 국문표기】	신동환
【성명의 영문표기】	SHIN, DONG-HWAN
【주민등록번호】	680925-1238825
【우편번호】	139-240
【주소】	서울특별시 노원구 공릉동 81 태강 아파트 1009-406
【국적】	KR
【발명자】	
【성명의 국문표기】	윤진호
【성명의 영문표기】	YOUN, JIN-HO
【주민등록번호】	660613-1905910
【우편번호】	140-729

【주소】 서울특별시 용산구 이촌2동(서부이촌동) 대림아파트 105 동 1803 호

【국적】 KR

【발명자】

【성명의 국문표기】 최영호

【성명의 영문표기】 CHOI, YOUNG-HO

【주민등록번호】 591209-1812444

【우편번호】 403-020

【주소】 인천광역시 부평구 산곡동 124-1 현대 5차 아파트 502-1008

【국적】 KR

【발명자】

【성명의 국문표기】 최종욱

【성명의 영문표기】 CHOI, JONG-UK

【주민등록번호】 520303-1812414

【우편번호】 142-090

【주소】 서울특별시 강북구 우이동 1 성원아파트 2-1301

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인 특허법인코리아나 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	12 면	12,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	13 항	525,000 원
【합계】		566,000 원
【감면사유】		중소기업
【감면후 수수료】		283,000 원

【첨부서류】 1. 요약서·명세서(도면)_1통 2. 중소기업기본법시행령 제2조에 의한 중소기업에 해당함을 증명하는 서류[사업자등록증사본, 원천징수이행상황신고서, 대차대조표]_2통

【요약서】**【요약】**

디지털 음성 저장장치 (DVR; Digital Voice Recorder) 에 저장된 데이터의 인증 및 위/변조를 방지하기 위한 장치 및 방법이 개시된다. 디지털 음성 저장장치 내 또는 디지털 음성 저장 장치와 접속되는 PC 내부에 위/변조 방지장치가 설치된다. 위/변조 방지 장치는 디지털 음성 저장장치에 오디오 데이터가 저장되기 전 또는 PC 내부의 데이터 저장부에 오디오 데이터가 저장되기 전에 데이터의 위/변조를 방지할 수 있는 처리를 수행한다. 이는 오디오 데이터에 워터마크를 삽입시킴에 의해, 오디오 데이터를 소정의 암호화키에 의해 암호화함에 의해, 또는 오디오 데이터에 해쉬값을 삽입시킴에 의해 이루어진다. 이에 따라, 디지털 음성 저장장치에 저장된 오디오 데이터의 위/변조 여부를 확인할 수 있다.

【대표도】

도 3

【색인어】

디지털 음성 저장장치, 워터마크, 암호화, 해쉬값

【명세서】**【발명의 명칭】**

디지털 음성 저장 장치에 저장된 데이터의 인증 및 위/변조를 방지하기 위한 장치 및 방법
{APPARATUS FOR AUTHENTICATION, PREVENTION OF FORGERY/ALTERATION OF THE DATA RECORDED BY
DIGITAL VOICE RECORDER AND METHOD THEREOF}

【도면의 간단한 설명】

도 1 은 일반적인 디지털 음성 저장 장치의 구성을 나타내는 블록도.

도 2 는 본 발명에 따른 위/변조 방지 장치가 디지털 음성 저장 장치 외부에 접속되는 구성을 나타내는 블록도.

도 3 은 본 발명에 따른 위/변조 방지 장치가 디지털 음성 저장 장치 내부에 배치되는 구성을 나타내는 블록도.

도 4a 는 본 발명의 제 1 실시예에 따른 워터마크의 삽입 및 검출 과정을 나타내는 도면

도 4b 는 본 발명의 제 1 실시예에 따른 워터마크 삽입장치의 구성을 나타내는 블록도.

도 5a 는 본 발명의 제 2 실시예에 따른 암호화 및 복호화 과정을 나타내는 도면.

도 5b 는 본 발명의 제 2 실시예에 따른 암호화 장치의 구성을 나타내는 블록도.

도 6a 는 본 발명의 제 3 실시예에 따른 해쉬함수를 이용한 데이터 인증과정을 나타내는 도면.

도 6b 는 본 발명의 제 3 실시예에 따른 해쉬값 삽입장치의 구성을 나타내는 도면.

※ 도면의 주요부분에 대한 부호의 설명※

201 : 마이크로폰 202 : 디지털 음성 저장장치

203 : 위/변조 방지장치 204 : 데이터 저장부

205 : PC 301 : 마이크로폰

3021 : A/D 변환장치

3022 : 중앙처리장치 또는 마이크로컨트롤로 (위/변조방지 장치)

3023 : D/A 변환장치 3024 : 스피커 또는 헤드폰

302 : 디지털 음성 저장장치 303 : PC

401 : 워터마크 삽입장치 402 : 워터마크 추출장치

411 : 아날로그 입력신호 412 : 입력신호 조절부

413 : A/D 변환장치

414 : 디지털 신호처리기 또는 마이크로컨트롤러

415 : D/A 변환장치 416 : 출력신호 조절부

417 : 아날로그 출력신호 418 : 데이터 압축/신장장치

501 : 암호화 장치 502 : 복호화 장치

511 : 입력신호 조절부 512 : A/D 변환 장치

513 : 디지털신호처리기 또는 마이크로컨트롤러

514 : 저장장치 515 : 전원공급장치

601 : 입력신호 조절부 602 : A/D 변환장치

603 : 디지털신호처리기 또는 마이크로컨트롤러

604 : 저장장치

605 : 전원공급장치

610 : 해쉬값 삽입장치

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<33> 본 발명은 디지털 음성 저장 장치 (Digital Voice Recorder; DVR) 에 저장된 데이터의 인증 및 위/변조를 방지하기 위한 장치 및 방법에 관한 것이다. 보다 상세하게는, 본 발명은 디지털 음성 저장 장치에 의하여 저장되는 데이터에 위/변조 방지장치를 사용하여 소정의 처리를 함으로써 저장된 데이터에 대하여 인증 및 위/변조를 방지하고, 위/변조가 된 경우 이를 확인할 수 있게 하는 장치 및 방법에 관한 것이다.

<34> 디지털 음성 저장 장치는 음성, 음향, 기타 소리를 디지털로 변환하여 플래쉬 메모리, DAT, 오디오 테이프 등과 같은 저장매체에 데이터를 저장하는 장치를 말한다.

<35> 도 1 은 일반적인 디지털 음성 저장 장치의 구성을 나타내는 블록도이다.

<36> 도 1 을 참조하면, 디지털 음성 저장장치 (100) 는 마이크로폰 (101), 입력신호 조절부 (102), 아날로그-디지털 변환장치 (103), 중앙처리장치 또는 마이크로컨트롤러 (104), 디지털-아날로그 변환장치 (105), 출력신호 조절부 (106), 스피커 또는 헤드폰 (107), 데이터 압축/신장 장치 (110), 데이터 저장장치 (111), 및 데이터 전송장치 (109) 를 포함하여 구성되며, 사용자의 필요에 따라 데이터 전송장치 (109) 를 통하여 PC (Personal Computer; 108) 와 접속될 수도 있다.

- <37> 마이크로폰 (101) 을 통하여 입력된 오디오 신호는 입력신호 조절부 (102) 에서 아날로그-디지털 변환장치 (103) 의 동작범위에 맞도록 조절된다. 아날로그-디지털 변환장치 (103) 에서는 입력된 아날로그 오디오 신호를 디지털 오디오 신호로 변환한다. 중앙처리장치 (CPU) 또는 마이크로컨트롤러 (104) 는 DVR 의 모든 동작을 제어하는 기능을 수행한다. 마이크로컨트롤러 (104) 는 그 내부에 프로그램 ROM, 데이터 RAM, CPU 등을 내장하여, 단독으로 DVR 의 동작 수행을 위한 프로그램을 실행시키는 칩을 말한다.
- <38> 데이터 압축/신장 장치 (110) 는 디지털 오디오 데이터를 압축하여 데이터 저장장치 (111) 에 저장하거나 데이터 저장장치 (111) 에서 압축된 디지털 데이터의 압축을 푸는 동작을 수행한다. 출력신호 조절부 (106) 는 디지털-아날로그 변환장치 (105) 를 통하여 변환된 아날로그 오디오 신호를 스피커 또는 헤드폰 입력에 맞도록 신호의 크기를 조절하는 부분이다. 스피커 또는 헤드폰 (107) 은 저장된 오디오 신호를 디지털 음성 저장장치 외부로 출력하는 장치이다.
- <39> 한편, 디지털 음성 저장장치에 저장된 데이터를 PC 로 전송하기 위하여 데이터 전송장치 (109) 가 사용된다. 데이터 전송장치 (109) 에는 직렬통신 (RS-232, USB, IEEE1394 등), 병렬통신 (PC 병렬 포트 통신 : SPP, ECP, EPP 등) 방법 등을 포함하는 PC 와 디지털 음성 저장장치를 접속시키는 통신수단을 구현하는 장치이다. PC (108) 는 디지털 음성 저장장치 (100) 에 저장된 데이터를 전송받는다. 전원공급장치 (112) 는 그 접속관계를 구체적으로 도시하지는 않았지만, 상술한 장치들에 전원을 공급하는 기능을 수행하며, 배터리 또는 AC-DC 컨버터 등으로 구현될 수 있다.
- <40> 상술한 디지털 음성 저장장치 (100) 의 동작을 개략적으로 살펴보면, 먼저 외부 오디오 신호가 마이크로폰 (101) 을 통하여 전기 신호로 변환되고, 입력신호 조절부 (102) 에서 아날

로그-디지털 변환장치 (103) 의 입력 범위에 맞게 조절된다. 조절된 오디오 신호는 아날로그-디지털 변환장치 (103) 에 의하여 디지털 오디오 신호로 변환된다. 오디오 신호의 저장을 위하여는, 디지털화된 오디오 신호는 중앙처리장치 또는 마이크로컨트롤러 (104) 에 의하여 데이터 압축/신장 장치 (110) 를 통하여 압축되어 데이터 저장장치 (111) 에 저장된다.

<41> 디지털 음성 저장장치 (100) 에 저장된 오디오 신호의 재생을 위하여는, 먼저 데이터 저장장치 (111) 에 저장된 오디오 신호를 데이터 압축/신장 장치 (110) 에서 압축을 풀고, 이를 디지털-아날로그 변환장치 (105) 에서 아날로그 신호로 변환하게 된다. 출력신호 조절부 (106) 는 아날로그화된 오디오 신호를 스피커 또는 헤드폰으로 출력하기 위한 적당한 신호 폭으로 변환하는 기능을 수행한다.

<42> 또한, PC (108) 로의 전송을 위하여는 오디오 신호의 재생 단계와 유사하게, 데이터 저장장치 (111) 로부터 데이터 압축/신장 장치 (110) 를 통하여 압축을 해제한다. 그 후, 이를 데이터 전송장치 (109) 를 통하여 PC (108) 로 전송하게 된다.

<43> 상술한 디지털 음성 저장장치는 대화 내용의 기록의 필요성이 있는 경우에 주로 사용된다. 예컨대, 회의 결과, 증권회사에서의 고객의 매도 및 매수 주문정보 등과 같은 추후에 분쟁의 소지가 있을 수 있는 대화 내용을 기록하는데 사용될 수도 있다.

<44> 그러나, 디지털 음성 저장장치를 점유하고 있는 일방과 그 상대방의 신뢰부족으로 인하여 디지털 음성 저장장치의 기록 내용에 대한 불신과 더불어, 저장된 오디오 데이터의 위/변조의 용이성으로 인하여, 이와 같이 저장된 오디오 데이터의 위/변조를 방지할 수 있는 보안 솔루션의 요청이 절실한 상태이다.



<45> 이와 관련하여, 종래에는 디지털 음성 저장장치에 저장된 오디오 데이터의 위/변조 문제에 관하여는 대책이 전무한 상태였다. 특히, 디지털 음성 저장장치가 대화 당사자 중 일방에게 그 지배권이 집중되어 있기 때문에, 타방 당사자가 그 진위 여부에 관하여 다룰 여지가 많았다.

【발명이 이루고자 하는 기술적 과제】

<46> 본 발명은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 본 발명에서는 디지털 음성 저장 장치에 저장된 데이터의 인증 및 위/변조를 방지하기 위한 장치, 즉 데이터의 위/변조를 추후 확인할 수 있게 해주는 워터마크 삽입 장치, 암호화 장치, 또는 해쉬값 삽입장치 등을 설치한다.

<47> 이에 따라, 디지털 음성 저장 장치에 데이터가 저장될 때 또는 디지털 음성 저장 장치로부터 PC 로 전송되어 저장될 때, 실시간으로 데이터의 위/변조를 방지 또는 확인할 수 있는 기술이 사용됨으로써, 디지털 음성 저장 장치에 저장되거나, 디지털 음성 저장 장치에 저장된 후 PC 로 전송된 데이터의 확인이 필요한 경우 저장된 데이터의 위/변조되었는지의 여부를 확인할 수 있는 장치 및 방법이 제공된다.

【발명의 구성 및 작용】

<48> 상술한 바와 같은 목적을 달성하기 위하여, 본 발명은 외부 오디오 데이터를 입력받는 오디오 데이터 입력부, 상기 오디오 데이터의 신호 크기를 조절하는 입력신호 조절부, 상기 오디오 데이터를 디지털로 변환하는 A/D 변환장치, 디지털 음성 저장장치의 동작을 제어하는 중앙처리장치 또는 마이크로컨트롤러, 상기 디지털화된 오디오 데이터를 압축하거나 압축된 오디오 데이터의 압축을 해제하는 데이터 압축/신장 장치, 및 상기 압축된 오디오 데이터를 저장하

는 데이터 저장장치를 구비하는 디지털 음성 저장장치에 저장된 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 위/변조 방지 장치로, 상기 A/D 변환 장치에 의하여 디지털화된 오디오 데이터가 상기 데이터 저장장치에 저장되기 전에 상기 오디오 데이터에 상기 위/변조를 방지하는 정보를 삽입하는 위/변조 방지장치를 제공한다.

<49> 바람직하게는, 상기 위/변조 방지장치는 범용 PCB 보드, DSP 칩보드, FPGA 보드, ASIC 보드, 또는 소프트웨어 프로그램의 형태로 상기 디지털 음성 저장 장치 내에서 구현된다.

<50> 또한, 본 발명은 오디오 데이터 입력부, 입력신호 조절부, A/D 변환장치, 중앙처리장치 또는 마이크로컨트롤러, 데이터 압축/신장 장치, 및 데이터 저장장치를 구비하는 디지털 음성 저장장치에 저장된 디지털화된 오디오 데이터를 전송받아 상기 오디오 데이터를 PC 에 저장하는 시스템에서, 상기 위/변조 방지 장치는 PC 내에 배치되고, 상기 위/변조 방지 장치는 상기 디지털화된 오디오 데이터가 상기 PC 내의 데이터 저장부에 저장되기 전에 상기 디지털화된 오디오 데이터에 상기 위/변조를 방지하는 정보를 삽입하는 상기 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 위/변조 방지 장치를 제공한다.

<51> 본 발명의 제 1 실시예에 따르면, 상기 위/변조를 방지하기 위한 정보의 삽입은 상기 오디오 데이터에 워터마크를 삽입함으로써 수행되고, 상기 워터마크의 확인은 상기 위/변조를 방지하기 위한 정보를 상기 워터마크의 검출을 통하여 수행된다. 여기서, 상기 워터마크는 강인한 워터마크 및 세미 워터마크 중 어느 하나이고, 상기 워터마크의 삽입은 상기 디지털화된 오디오 데이터를 압축하기 전에 수행되는 것이 바람직하다. 대체적으로는, 상기 워터마크는 연약한 워터마크이고, 상기 워터마크의 삽입은 상기 디지털화된 오디오 데이터를 압축한 후에 수행되는 것이 바람직하다.

- <52> 본 발명의 제 2 실시예에 따르면, 상기 위/변조를 방지하기 위한 정보의 삽입은 상기 오디오 데이터를 소정의 암호화키에 의해 암호화함으로써 수행된다.
- <53> 본 발명의 제 3 실시예에 따르면, 상기 위/변조를 방지하기 위한 정보의 삽입은 상기 오디오 데이터에 상기 오디오 데이터의 해쉬값을 삽입시킴으로써 수행되고, 상기 저장된 오디오 데이터의 위/변조 여부의 확인은 상기 저장된 오디오 데이터에 삽입되어 있는 해쉬값과 상기 저장된 오디오 데이터를 상기 해쉬값을 얻기 위하여 사용한 해쉬함수에 적용시켜 새롭게 구한 해쉬값의 동일성 여부의 확인으로서 수행된다.
- <54> 본 발명의 다른 목적을 달성하기 위하여, 본 발명은 오디오 데이터 입력부, 입력신호 조절부, A/D 변환장치, 중앙처리장치 또는 마이크로컨트롤러, 데이터 압축/신장 장치, 및 데이터 저장장치를 구비하는 디지털 음성 저장장치에 저장된 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 방법으로서, (a) 상기 A/D 변환장치에 의하여 디지털화된 오디오 데이터를 수신하는 단계; (b) 상기 디지털화된 오디오 데이터에 상기 위/변조를 방지하기 위한 정보를 실시간으로 삽입하는 단계; 및 (c) 상기 위/변조 방지 정보가 삽입된 상기 오디오 데이터를 저장하는 단계를 포함하는 방법을 제공한다.
- <55> 한편, 본 발명은 오디오 데이터 입력부, 입력신호 조절부, A/D 변환장치, 중앙처리장치 또는 마이크로컨트롤러, 데이터 압축/신장 장치, 및 데이터 저장장치를 구비하는 디지털 음성 저장장치에 저장된 디지털화된 오디오 데이터를 전송받아 상기 오디오 데이터를 PC 에 저장하는 시스템에서, 상기 PC 내에서 상기 전송받은 오디오 데이터에 상기 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 방법으로서, (a) 상기 디지털 음성 저장장치에 저장된 디지털화된 오디오 데이터를 수신하는 단계; (b) 상기 디지털화된 오디오 데이터에 상기 위/변조를 방

지하기 위한 정보를 실시간으로 삽입하는 단계; 및 (c) 상기 위/변조 방지 정보가 삽입된 상기 오디오 데이터를 저장하는 단계를 포함하는 방법을 제공한다.

<56> 본 발명의 제 1 실시예에 따르면, 상기 (b) 단계는 상기 오디오 데이터에 워터마크를 삽입함으로써 수행되고, 상기 위/변조를 방지하기 위한 정보의 확인은 상기 워터마크의 검출을 통하여 수행된다.

<57> 본 발명의 제 2 실시예에 따르면, 상기 (b) 단계는 상기 오디오 데이터를 소정의 암호화 키에 의해 암호화함으로써 수행된다.

<58> 본 발명의 제 3 실시예에 따르면, 상기 (b) 단계는 상기 오디오 데이터에 상기 오디오 데이터의 해쉬값을 삽입시킴으로써 수행되고, 상기 저장된 오디오 데이터의 위/변조 여부의 확인은 상기 저장된 오디오 데이터에 삽입되어 있는 해쉬값과 상기 저장된 오디오 데이터를 상기 해쉬값을 얻기 위하여 사용한 해쉬함수에 적용시켜 새롭게 구한 해쉬값의 동일성 여부의 확인으로서 수행된다.

<59> 이하, 첨부되는 도면을 참조로 하여 본 발명의 바람직한 실시예에 대하여 상술하기로 한다.

<60> 우선, 본 발명에 따른 위/변조장치 (이는 구체적으로는 워터마크 삽입 장치, 암호화 장치, 또는 해쉬값 삽입장치가 될 수 있으며, 이에 대해서는 도 4 내지 도 6 을 참조로 하여 후에 상세히 설명한다) 가 디지털 음성 저장 장치의 여러 실시예에 적용되는 구성에 대하여 도 2 및 도 3 을 참조로 하여 설명한다.

<61> 도 2 는 본 발명에 따른 위/변조 방지 장치가 디지털 음성 저장 장치 외부에 접속되는 구성을 나타내는 블록도이다.

- <62> 도 2 를 참조로 하면, 위/변조 방지 장치 (203) 가 PC (205) 내에 배치되어 있으며, 디지털 음성 저장장치 (202) 로부터 전송된 데이터에 위/변조 방지 수단을 삽입하게 된다.
- 위/변조 방지 장치 (203) 의 동작을 보다 구체적으로 설명하면, 먼저, 마이크로폰 (201) 으로부터 오디오 신호가 입력된다. 입력된 오디오 신호는 디지털화되어 디지털 음성 저장 장치 (202) 에 저장되며, 영구적인 보관 또는 필요에 따라서 데이터 전송장치 (109) 를 통하여 이를 PC (205) 로 업로드 (upload) 한다. 이 때, PC (205) 내에 설치된 위/변조 방지장치 (203) 에서 소정의 위/변조 방지 수단을 삽입한다. 위/변조 방지 장치 (203) 는 저장될 데이터에 인증정보를 삽입하는 부분으로, 나중에 저장된 데이터의 위/변조 여부를 판별하고자 할 때, 삽입된 정보를 이용하여 위/변조 여부를 판별하게 된다. 그 후, 오디오 데이터는 PC (205) 내부의 하드디스크 드라이브와 같은 소정의 저장매체 (데이터 저장부; 204) 에 저장된다.
- <63> 상기 위/변조 방지 장치 (203) 는 워터마크 삽입 장치, 암호화 장치, 또는 해쉬값 삽입 장치가 될 수 있으며, 이에 대하여는 도 4 내지 도 6 을 참조로 하여 상세히 후술한다.
- <64> 도 3 은 본 발명에 따른 위/변조 방지 장치가 디지털 음성 저장 장치 내부에 배치되는 구성을 나타내는 블록도이다.
- <65> 도 3 을 참조하여, 마이크로폰 (301) 으로부터 입력되는 오디오 신호가 디지털화되어 디지털 음성 저장장치 (302) 의 데이터 저장장치 (3024) 에 저장되기에 앞서, 위/변조 방지장치 (3022) 에서 상기 오디오 신호에 위/변조를 방지하기 위한 정보가 삽입된다. 그 후, 오디오 신호는 PC (303) 로 전송되어, PC (303) 에 저장될 수도 있다.
- <66> 도 3 에서는 본 발명에 따라서 디지털 음성 저장 장치 내부에 배치되는 위/변조 방지 장치 (3022) 를 중앙처리장치 (CPU) 또는 마이크로컨트롤러 (104) 에서 그 동작을 수행하도록 구



현하였지만, 당업자는 상기 위/변조 방지 장치 (3022) 가 별도의 장치로써 구현될 수도 있음은 물론이다.

- <67> 디지털 음성 저장장치 (302) 내에 포함된 위/변조 방지 장치는 워터마크 삽입 장치, 암호화 장치, 또는 해쉬값 삽입 장치가 될 수 있으며, 이에 대하여는 도 4 내지 도 6 을 참조로 하여 상세히 후술한다.
- <68> 도 2 및 도 3 에서의 위/변조 방지 장치 (203, 3022) 는 범용 PCB 보드, DSP 칩보드, FPGA (Flexible Program Gate Array) 보드, ASIC (Application Specific Integrated Circuit) 보드, 또는 소프트웨어 프로그램의 형태로 구현될 수도 있다.
- <69> 이하에서는 상술한 위/변조 방지 장치 (203, 3022) 에서 사용된 본 발명의 바람직한 제 1, 제 2, 및 제 3 실시예에 따른 구체적인 위/변조 방지 기술 및 상기 위/변조 방지장치 (203, 3022) 의 내부 구성에 대하여 설명한다.
- <70> 본 발명의 제 1 실시예는 워터마킹 방법에 의한 위/변조 방지 장치의 구현이다.
- <71> 도 4a 는 본 발명의 제 1 실시예에 따른 워터마크의 삽입 및 검출 과정을 나타내는 도면이다.
- <72> 도 4a 를 참조하면, 워터마크 삽입장치 (401) 에서는 입력된 오디오 신호에 워터마크를 삽입한다. 삽입되는 워터마크 정보는 추후 오디오 데이터의 진위를 증명할 수 있는 정보이다. 워터마크 삽입장치 (401) 는 상술한 본 발명의 위/변조 방지장치를 의미한다. 이후, 워터마크가 삽입된 오디오 데이터는 저장장치에 저장됨으로써, 본 발명에 따른 위/변조를 방지할 수 있는 정보의 삽입 과정은 종료된다.

- <73> 본 실시예에서 사용될 수 있는 워터마크의 유형으로는 강인한 워터마크 (RW : Robust Watermark), 세미 워터마크 (SFW : Semi-Fragile Watermark), 및 연약한 워터마크 (FW : Fragile Watermark) 가 있고, 이들은 외부적인 공격 또는 변형에 워터마크가 견디는 정도에 따른 구분이다.
- <74> 강인한 워터마크는 압축과 A/D 변환, D/A 변환, 잡음 첨가 등과 같은 공격에도 워터마크 정보를 추출할 수 있는 워터마크를 의미한다. 세미 워터마크는 압축과 같은 정도의 공격에는 워터마크가 살아남고, 오디오 데이터를 변조시키는 악의적인 공격에는 워터마크가 깨지는 특성을 갖고 있다. 연약한 워터마크는 약간의 변형에도 워터마크가 깨지는 특성을 가지고 있다. 따라서, 본 발명에서 연약한 워터마크를 사용할 경우에는, 데이터의 압축 저장시 오디오 데이터의 압축 후에 워터마크를 삽입하여야 한다.
- <75> 비록 도 4a 에서는 연속적인 과정으로 도시하였지만, 본 발명에 따라 이와 같이 위/변조 방지장치에서 워터마크가 삽입된 오디오 데이터는 추후 데이터의 위/변조 여부가 문제되었을 경우, 별도의 오프라인상의 워터마크 추출장치 (PC 상에 구현되는 소프트웨어 프로그램일 수도 있다.) 에서 워터마크의 추출 과정이 수행되는 것이 일반적이다. 상기 워터마크의 추출은 워터마크로서 삽입된 정보 자체의 인증일 수도 있으며, 또한 워터마크가 깨졌는지 여부에 의한 저장된 오디오 데이터의 위/변조 여부의 확인일 수도 있다.
- <76> 도 4b 는 본 발명의 제 1 실시예에 따른 워터마크 삽입장치의 구성을 나타내는 블록도이다. 즉, 도 2 내지 도 3 의 위/변조 방지장치가 본 발명의 제 1 실시예에 따라 워터마크 삽입장치로서 구현된 것이다.
- <77> 도 4b 를 참조하면, 본 발명의 제 1 실시예에 따른 워터마크 삽입장치 (401) 는 입력 신호 조절부 (412), 아날로그-디지털 변환장치 (413), 디지털신호처리기 또는 마이크로컨트롤러

(414), 디지털-아날로그 변환장치 (415), 출력신호 조절부 (416), 및 전원공급장치 (418) 를 포함하여 구성된다.

<78> 입력신호 조절부 (412) 에서는 상술한 마이크로폰으로부터 입력되는 아날로그 입력신호 (401 : 오디오 신호) 를 A/D 변환장치 (413) 의 입력 범위에 맞도록 조절해준다. 조절된 아날로그 오디오 신호는 A/D 변환장치 (413) 에 의하여 디지털 오디오 신호로 변환된다.

<79> 변환된 오디오 신호는 디지털 신호처리기 또는 마이크로컨트롤러 (414) 에서 워터마크가 삽입되고, 워터마크가 삽입된 오디오 신호는 D/A 변환장치 (415) 에서 다시 아날로그 신호 (즉, 오디오 신호) 로 변환되고, 그 후 워터마크가 삽입된 상기 아날로그 신호는 출력신호 조절부 (416) 에서 소정의 범위로 그 출력이 조절되어, 아날로그 출력신호 (417) 가 출력된다. 한편, 전원공급장치 (418) 는 디지털 신호처리기 또는 마이크로컨트롤러 (414) 에 필요한 전력을 공급하여 준다.

<80> 한편, 사용하고자 하는 워터마크가 강인한 워터마크이거나 세미 워터마크인 경우에는, 워터마크의 삽입은 상기 디지털화된 오디오 데이터를 압축하기 전에 수행되는 것이 바람직하다. 대체적으로, 사용하고자 하는 워터마크가 연약한 워터마크인 경우에는, 워터마크의 삽입은 상기 디지털화된 오디오 데이터를 압축한 후에 수행되는 것이 바람직하다.

<81> 본 발명의 제 2 실시예는 암호화 알고리즘의 사용에 의한 위/변조 방지장치의 구현이다.

<82> 도 5a 는 본 발명의 제 2 실시예에 따른 암호화 및 복호화 과정을 나타내는 도면이다.

<83> 도 5a 를 참조로 하면, 암호화장치 (501) 에서는 입력된 오디오 데이터를 소정의 암호화 알고리즘에 의해서 암호화한다. 이 때, 암호화에는 소정의 암호화키가 사용된다. 암호화된 데이터는 데이터 저장장치 (미도시) 에 저장된다.



- <84> 본 발명에 따라 이와 같이 위/변조 방지장치에서 소정의 암호화키에 의해 암호화된 오디오 데이터는 추후 데이터의 위/변조 여부가 문제되었을 경우, 별도의 오프라인상의 복호화 장치 (PC 상에 구현되는 소프트웨어 프로그램일 수도 있음) 에서 암호화된 데이터의 복호화 과정을 수행함으로써, 저장된 오디오 데이터의 위/변조 여부의 확인이 가능하다.
- <85> 본 발명의 바람직한 실시예에 따른 암호화 시스템의 유형으로는 대칭키 암호화 시스템 (Symmetric Cryptosystem : 공개키 암호화 시스템이라고도 함) 및 비대칭키 암호화 시스템 (Asymmetric Cryptosystem : 비밀키 암호화 시스템이라고도 함) 이 있다. 대칭키 암호화 시스템은 암호화키와 복호화키가 동일한 것이며, 비대칭키 암호화 시스템은 암호화키와 복호화키가 서로 상이한 것이다.
- <86> 대칭키 암호화 알고리즘은 암호화 및 복호화 속도가 빠른 특성이 있으며, DES, 3DES, SEED, 및 Rijndael 등이 이에 포함된다. 비대칭키 암호화 알고리즘은 수학적으로 풀기 어렵고 복호화 시간이 많이 걸린다는 특성이 있으며, RSA, ElGamal, 및 ECC 등이 이에 포함된다. 본 발명에서는 어떠한 암호화 알고리즘을 사용하여도 무방하다.
- <87> 본 발명의 바람직한 실시예에서는 미국의 NIST 에 의해서 AES (Advanced Encryption Standard) 로서 채택된 128 비트 Rijndael 알고리즘을 사용하여 실험을 하였으며 그 실험 결과를 아래에 나타냈다. 하기의 실험결과는 미국의 TI DSP (TI Digital Signal Processor) 를 사용하여 Rijndael 알고리즘을 구현하였을 때의 256 바이트의 암호화된 데이터를 256 바이트의 복호화된 원 데이터 (Raw Data) 로 만드는데 소요된 자원 (Resource) 을 나타낸다.
- <88> * TI DSP (TMS 320VC5410) 에서 복호화시킬 때 사용된 리소스 : 256 Byte
- <89> * 연산용량 : 약 20 MIPS (Million Instruction Per Second)

- <90> * TI DSP 에서 복호화시킬때 사용되는 프로그램 코드 메모리 크기 : 10 KB (10,714 Byte)
- <91> * TI DSP 에서 복호화시킬 때 사용되는 데이터 메모리 크기 : 1KB (1024 Byte)
- <92> 도 5b 는 본 발명의 제 2 실시예에 따른 암호화 장치 (501) 의 구성을 나타내는 블록도로서, 도 4b 와는 다르게 디지털 신호처리기 또는 마이크로컨트롤러 (513) 가 워터마크를 삽입하는 기능을 수행하는 것이 아니라, 디지털 오디오 데이터를 암호화키를 사용하여 암호화하는 기능을 수행한다는 점을 제외하고는 도 4b 에서의 설명이 동일하게 적용된다.
- <93> 본 발명의 제 3 실시예는 해쉬함수를 사용하는 위/변조 방지장치의 구현이다.
- <94> 도 6a 는 본 발명의 제 3 실시예에 따른 해쉬함수를 이용한 데이터 인증과정을 설명하는 도면이다.
- <95> 도 6a 를 참조하면, 입력된 오디오 데이터는 해쉬함수에 입력되고, 이는 하기의 수학식 1 로서 나타낼 수 있다. 사용가능한 해쉬함수로는 바람직하게는 MD5 (Message Digest 5) 가 사용되나 이에 제한되는 것은 아니다.
- <96> 【수학식 1】 $M_1 = H(I)$
- <97> 여기에서, I 는 입력데이터이고, H(x) 는 해쉬함수, M_1 은 계산된 해쉬값이다.
- <98> 해쉬함수의 출력값인 해쉬값 (M_1) 이 입력 오디오 데이터에 삽입되고, 오디오 데이터는 해쉬값 (M_1) 이 삽입된 상태로 저장매체에 저장된다.
- <99> 해쉬함수의 특징은 단방향 함수라는 것에 있다. 즉, 해쉬값만을 가지고 해쉬함수에 입력된 입력데이터를 추론할 수는 없다.

- <100> 본 발명에 따라 이와 같이 위/변조 방지장치에서 소정의 해쉬함수에 의해 계산된 해쉬값이 삽입된 오디오 데이터는 추후 데이터의 위/변조 여부가 문제되었을 경우, 별도의 오프라인상의 해쉬값 인증장치 (PC 상에 구현되는 소프트웨어 프로그램일 수도 있다.) 에서 해쉬값의 인증 과정을 수행함으로써, 저장된 오디오 데이터의 위/변조 여부의 확인이 가능하다.
- <101> 해쉬값 인증의 구체적인 과정은 다음과 같다. 저장된 오디오 데이터는 입력 오디오 데이터 자체와 그 데이터에 해쉬함수를 적용하여 계산된 해쉬값 (M_1) 으로 이루어진다. 입력 데이터에 해쉬값 삽입장치 (즉, 본 발명에 따른 위/변조 방지장치) 에서 사용한 것과 동일한 해쉬함수를 이용하여 새로운 해쉬값 (M_2) 을 구한다. 만약, 저장된 오디오 데이터에 삽입되어 있는 해쉬값 (M_1) 과 새롭게 구한 해쉬값 (M_2) 가 서로 동일하다면 저장된 오디오 데이터는 위/변조되지 않은 원본인 것이고, 만약 두 해쉬값이 서로 다르다면 상기 저장된 오디오 데이터는 위/변조된 것으로 판단된다.
- <102> 도 6b 는 본 발명의 제 3 실시예에 따른 해쉬값 삽입장치 (610) 의 구성을 나타내는 도면으로서, 도 4b 와는 다르게 디지털 신호처리기 또는 마이크로컨트롤러 (603) 가 워터마크를 삽입하는 기능을 수행하는 것이 아니라 디지털 오디오 데이터에 대한 해쉬값을 계산하고, 그 계산된 해쉬값을 오디오 데이터의 특정부분에 삽입하는 기능을 수행한다는 점을 제외하고는 도 4b 에서의 설명이 동일하게 적용된다.
- <103> 본 발명을 상기 실시예들을 참조하여 특별히 도시하고 설명하였지만, 이는 단지 예시를 위하여 사용한 것이며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 첨부되는 특허 청구범위에서 정의한 것과 같이 본 발명의 기술적 사상 및 범위를 벗어나지 않고 다양한 변형을 할 수 있음을 알 수 있다.

【발명의 효과】

<104> 상술한 바와 같은 본 발명에 따르면, 디지털 음성 저장장치 (DVR : Digital Voice Recorder) 에 통화 데이터가 저장될 때 실시간으로 데이터의 위/변조를 방지 또는 확인할 수 있는 기술을 사용함으로써, 저장된 오디오 데이터의 확인이 필요한 경우, 저장된 오디오 데이터가 위/변조되었는지의 여부를 확인할 수 있는 효과가 있다.

【특허청구범위】**【청구항 1】**

오디오 데이터 입력부, 상기 오디오 데이터 입력부에서 입력된 아날로그 오디오 데이터를 디지털화하는 A/D 변환장치, 및 상기 디지털화된 오디오 데이터를 저장하는 데이터 저장장치를 구비하는 디지털 음성 저장장치에 저장되는 오디오 데이터에 위/변조를 방지하는 정보를 삽입하는 위/변조 방지 장치에 있어서,

상기 위/변조 방지 장치는 상기 A/D 변환장치에서 디지털화된 오디오 정보를 상기 A/D 변환장치로부터 수신하여, 상기 디지털화된 오디오 데이터가 상기 데이터 저장장치에 저장되기 전에 상기 오디오 데이터에 상기 위/변조를 방지하는 정보를 삽입하는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 2】

디지털 음성 저장장치에 저장된 디지털화된 오디오 데이터를 전송받아 상기 오디오 데이터를 PC 에 저장하는 시스템에서, 상기 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 위/변조 방지 장치로서,

상기 위/변조 방지 장치는 PC 내에 배치되고,

상기 위/변조 방지 장치는 상기 디지털화된 오디오 데이터가 상기 PC 내의 데이터 저장부에 저장되기 전에 상기 디지털화된 오디오 데이터에 상기 위/변조를 방지하는 정보를 삽입하는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 위/변조를 방지하기 위한 정보의 삽입은 상기 오디오 데이터에 워터마크를 삽입함으로써 수행되고,

상기 저장된 오디오 데이터의 위/변조 여부의 확인은 상기 워터마크의 검출을 통하여 수행되는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 4】

제 1 항 또는 제 2 항에 있어서,

상기 위/변조를 방지하기 위한 정보의 삽입은 상기 오디오 데이터를 소정의 암호화키에 의해 암호화함으로써 수행되는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 5】

제 1 항 또는 제 2 항에 있어서,

상기 위/변조를 방지하기 위한 정보의 삽입은 상기 오디오 데이터에 상기 오디오 데이터의 해쉬값을 삽입시킴으로써 수행되고,

상기 저장된 오디오 데이터의 위/변조 여부의 확인은 상기 저장된 오디오 데이터에 삽입되어 있는 해쉬값과 상기 저장된 오디오 데이터를 상기 해쉬값을 얻기 위하여 사용한 해쉬함수에 적용시켜 새롭게 구한 해쉬값의 동일성 여부의 확인으로서 수행되는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 6】

제 1 항에 있어서,

상기 위/변조 방지장치는 범용 PCB 보드, DSP 칩보드, FPGA 보드, ASIC 보드, 또는 소프트웨어 프로그램의 형태로 상기 디지털 음성 저장 장치 내에서 구현되는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 7】

제 3 항에 있어서,

상기 워터마크는 강인한 워터마크 및 세미 워터마크 중 어느 하나이고,

상기 워터마크의 삽입은 상기 디지털화된 오디오 데이터를 압축하기 전에 수행되는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 8】

제 3 항에 있어서,

상기 워터마크는 연약한 워터마크이고,

상기 워터마크의 삽입은 상기 디지털화된 오디오 데이터를 압축한 후에 수행되는 것을 특징으로 하는 위/변조 방지 장치.

【청구항 9】

오디오 데이터 입력부, 상기 오디오 데이터 입력부에서 입력된 아날로그 오디오 데이터를 디지털화하는 A/D 변환장치, 및 상기 디지털화된 오디오 데이터를 저장하는 데이터 저장장치를 구비하는 디지털 음성 저장장치에 저장된 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 방법에 있어서,

(a) 상기 A/D 변환장치에 의하여 디지털화된 오디오 데이터를 수신하는 단계;

(b) 상기 디지털화된 오디오 데이터에 상기 위/변조를 방지하기 위한 정보를 실시간으로 삽입하는 단계; 및

(c) 상기 위/변조 방지 정보가 삽입된 상기 오디오 데이터를 저장하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 10】

디지털 음성 저장장치에 저장된 디지털화된 오디오 데이터를 전송받아 상기 오디오 데이터를 PC 에 저장하는 시스템에서, 상기 PC 내에서 상기 전송받은 오디오 데이터에 상기 오디오 데이터의 위/변조를 방지하는 정보를 삽입하는 방법으로서,

(a) 상기 디지털 음성 저장장치에 저장된 디지털화된 오디오 데이터를 수신하는 단계;

(b) 상기 디지털화된 오디오 데이터에 상기 위/변조를 방지하기 위한 정보를 실시간으로 삽입하는 단계; 및

(c) 상기 위/변조 방지 정보가 삽입된 상기 오디오 데이터를 저장하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 11】

제 9 항 또는 제 10 항에 있어서,

상기 (b) 단계는 상기 오디오 데이터에 워터마크를 삽입함으로써 수행되고,

상기 저장된 오디오 데이터의 위/변조 여부의 확인은 상기 워터마크의 검출을 통하여 수행되는 것을 특징으로 하는 방법.

【청구항 12】

제 9 항 또는 제 10 항에 있어서,

상기 (b) 단계는 상기 오디오 데이터를 소정의 암호화키에 의해 암호화함으로써 수행되는 것을 특징으로 하는 방법.

【청구항 13】

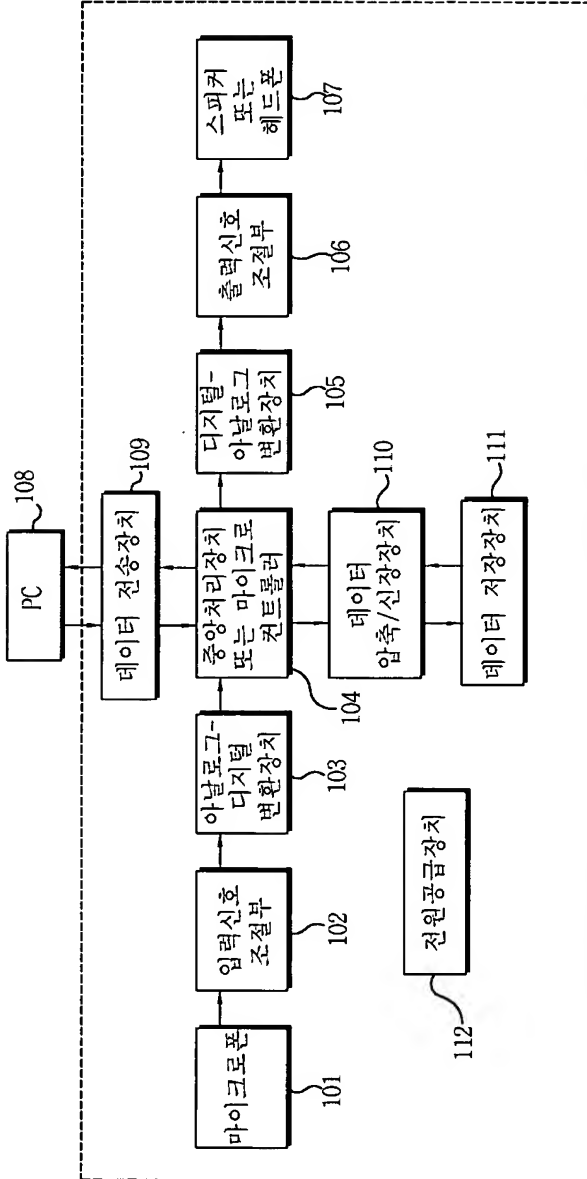
제 9 항 또는 제 10 항에 있어서,

상기 (b) 단계는 상기 오디오 데이터에 상기 오디오 데이터의 해쉬값을 삽입시킴으로써 수행되고,

상기 저장된 오디오 데이터의 위/변조 여부의 확인은 상기 저장된 오디오 데이터에 삽입되어 있는 해쉬값과 상기 저장된 오디오 데이터를 상기 해쉬값을 얻기 위하여 사용한 해쉬함수에 적용시켜 새롭게 구한 해쉬값의 동일성 여부의 확인으로서 수행되는 것을 특징으로 하는 방법.



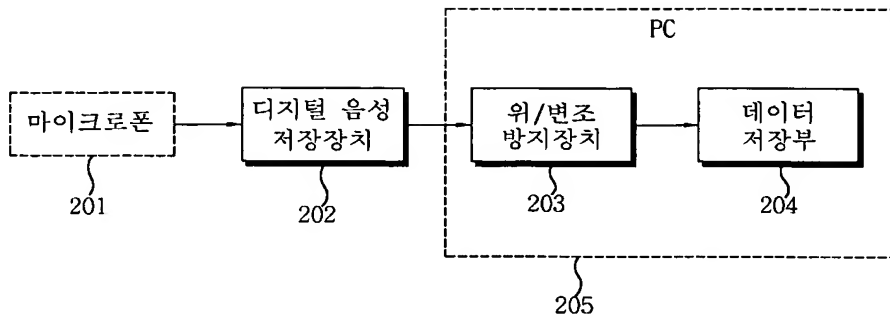
【도 1】



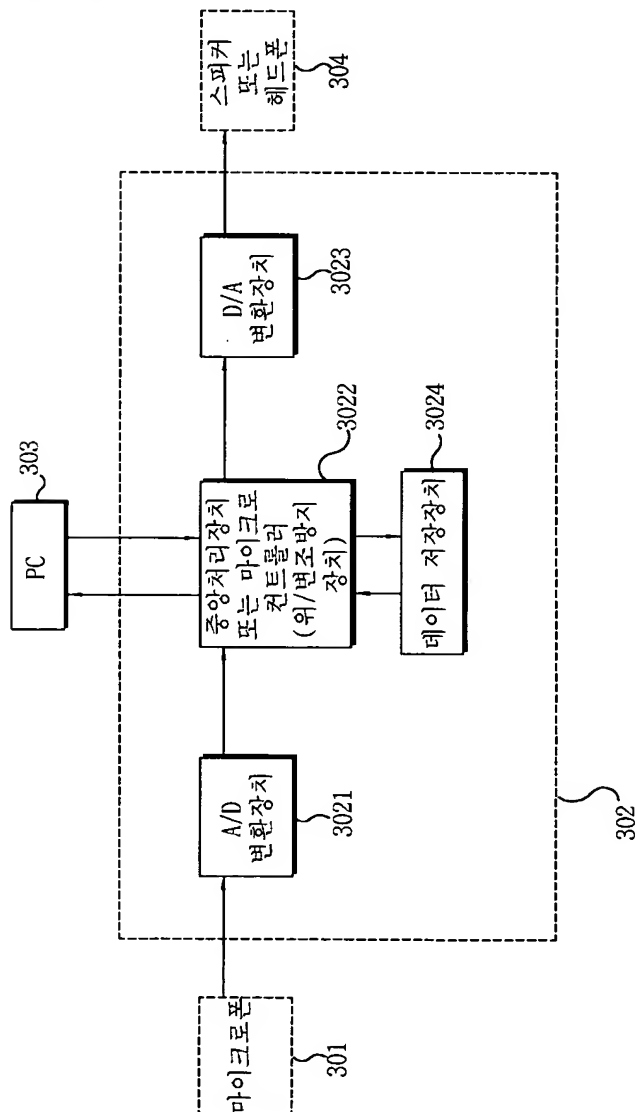
【도면】



【도 2】

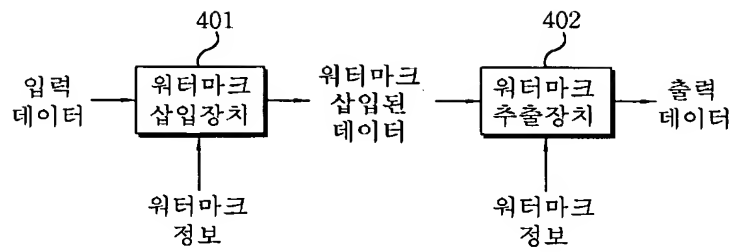


【도 3】

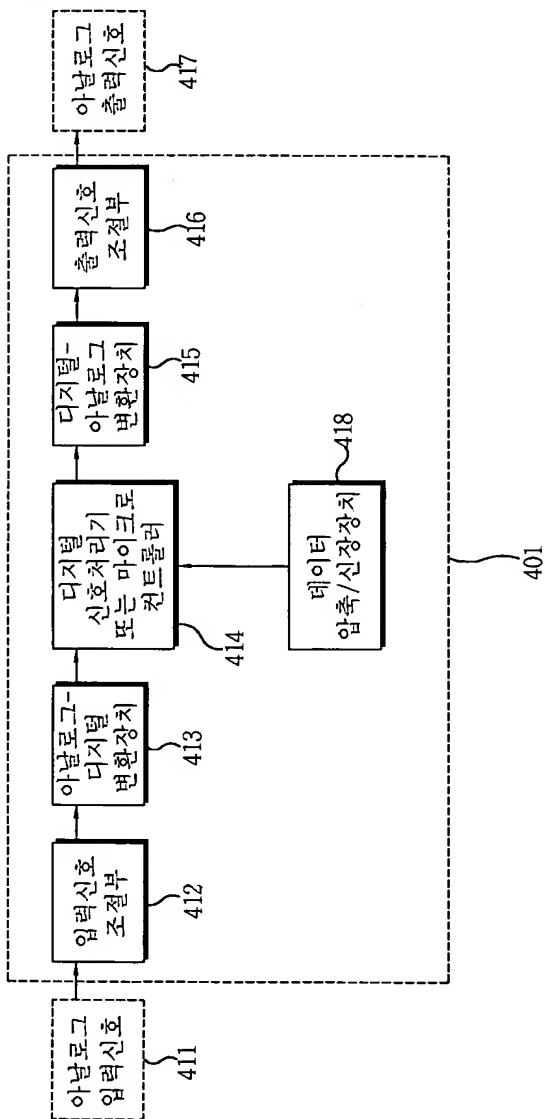




【도 4a】

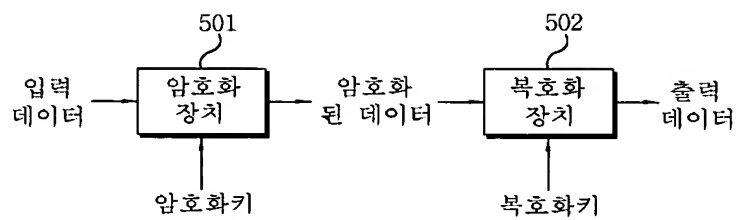


【도 4b】

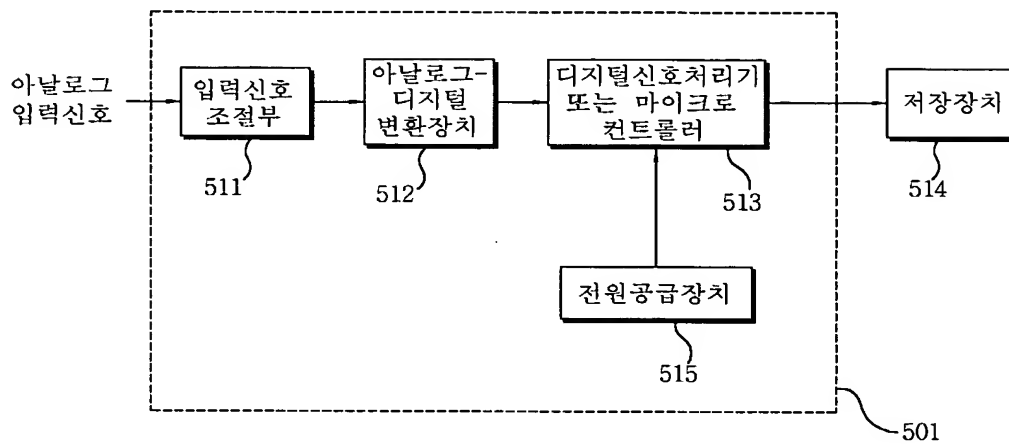




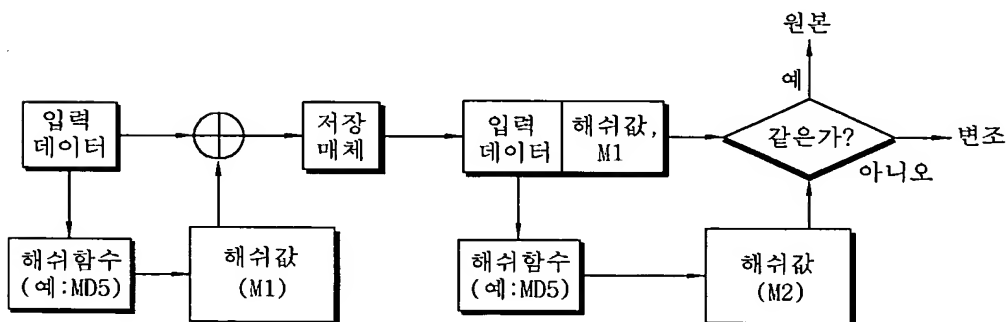
【도 5a】



【도 5b】



【도 6a】



【도 6b】

